PATENTS
Attorney Docket No. SMY-219.01
P4421

REMARKS

In this Response, Applicants cancel claims 2, 3, 11, and 14, amend claims 1, 4, 7, 8, 10, 12, 13, 15-17, 20-24, 26, 31, and 35-37, and remove the bases for the Examiner's rejections. Applicants amend the claims solely to expedite prosecution and do not acquiesce to any of the Examiner's rejections. Applicants' amendments to the claims are supported throughout the application. Applicants' silence with regard to the Examiner's rejections of dependent claims constitutes a recognition by the Applicants that the rejections are moot based on the Amendment and/or Remarks relative to the independent claim from which the dependent claims depend. Applicants reserve the option to further prosecute the same or similar claims in the present or a subsequent application. Upon entry of the Amendment, claims 1, 4-10, 12, 13, and 15-37 are pending in the present application.

Extension of Time

As provided in accompanying documents, Applicants request a one-month extension of time under 37 C.F.R. § 1.136(a) in which to file this Response.

Claim Rejections

35 U.S.C. § 112, ¶ 2

The Examiner rejected claim 17 for being dependent on itself. In reply, Applicants amend claim 17 to be dependent on 13. This amendment removes the basis for the Examiner's rejection of claim 17.

35 U.S.C. §§ 102(b) and 103(a)

The Examiner rejected all of the pending claims under 35 U.S.C. § 102(b) and/or 35 U.S.C. § 103(a). Most relevantly, the Examiner rejected independent claims 1, 13, 31, and 35-37 under § 102(b) as being anticipated by Ganesan, independent claim 20 under § 102(b) as being

anticipated by Eldridge, and independent claim 21 under § 103(a) as being unpatentable over Eldridge in view of Ganesan..

Claims 1, 4-10, and 12

Independent claim 1 describes a method by which an entity can store information on an otherwise non-secure server (e.g., a file server) so that only authorized users (e.g., a client) can access it. In accordance with claim 1, a file server stores information encrypted with a first encryption key and uses an access-control list to control access to the encrypted information. The access-control list includes an entry having (a) an identifier for a client that is authorized to at least read the information and (b) a first decryption key that is usable to decrypt the encrypted information and that is encrypted with a second encryption key. The second encryption key is associated with a second decryption key that is accessible to the client and that is usable to decrypt the encrypted first decryption key. In response to a request from the client, the file server transmits the encrypted information and the entry (i.e., the client identifier and the encrypted first decryption key) to the client.

Ganesan teaches data transmission and data storage scenarios. In contrast to independent claim 1, Ganesan does not teach or suggest transmitting, in response to a request from a client, (i) information that is encrypted with a first encryption key and (ii) a first decryption key that is usable to decrypt the encrypted information and that is itself encrypted with a second encryption key, in which the second encryption key is associated with a second decryption key that is accessible to the client and that is usable to decrypt the encrypted first encryption key.

In Ganesan's data transmission scenarios, a client 110 sends to a client 140 a message including (i) data encrypted with a symmetric session key and (ii) the symmetric session key encrypted with client 140's public key. (Ganesan col. 9, l. 47 to col. 10, l. 28.) True, a router that is located between client 110 and client 140 may briefly store the message prior to transmitting it to client 140. Even if Ganesan's transmission scenarios do thereby suggest the *storing* feature of claim 1, however, they do not teach or suggest the *transmitting* feature of claim 1 because the router does not transmit the encrypted data and the encrypted session key to client

140 *in response to a request from client 140*. Rather, the router transmits the message to client 140 only on the request of client 110, and independently of a request from client 140.

In Ganesan's data storage scenarios, a client 110 sends to file server 150 a message including data to be stored on file server 150 and an encrypted symmetric key, which symmetric key can be decrypted only by file server 150. (Ganesan col. 10, l. 30 to col. 11, l. 35.) In response, file server 150 saves a copy of the encrypted symmetric key, uses the file server's private key to decrypt the encrypted symmetric key, and uses the revealed symmetric key to encrypt the stored data. File server 150 thus stores (i) data encrypted with a symmetric key and (ii) the symmetric key encrypted with the file server's public key. The data is not, however, encrypted in the manner claimed in claim 1 because the symmetric key which encrypts the data is not itself encrypted so that it can be decrypted by client 110 or another client who might request that data. Since the symmetric key is encrypted with the file server's public key, and since the file server's private key is accessible only to the file server, the symmetric key can be decrypted only by file server 150, and not by client 110. Ganesan's storage scenarios do not, therefore, encrypt the data stored on file server 150 in the manner claimed in claim 1. As such, Ganesan's storage scenarios do not teach or suggest the *storing* feature of claim 1. Since they do not do not teach or suggest the *storing* feature of claim 1, and since the transmitting feature of claim 1 transmits the thusly stored data, they do not teach or suggest the *transmitting* feature of claim 1.

In summary, neither Ganesan's transmission scenarios nor Ganesan's storage scenarios teach or suggest the feature of claim 1 directed to *transmitting the encrypted information and the entry to the client in response to a request from the client.*

Independent claim 1 is, therefore, allowable. Since claim 1 is allowable, claims 4-10 and 12 depending therefrom are also allowable.

Claims 13, 15-19, and 31-37

Independent claims 13, 31, and 34-37 include features similar to those in independent claim 1. Since independent claim 1 is allowable, independent claims 13, 31, and 34-37 and claims 15-19, 32, and 33 depending therefrom are also allowable.

Claims 21-30

Independent claims 20 and 21 describe data storage methods in which a file server stores information for members of a group such that (a) the stored information is encrypted with a first encryption key, (b) a first decryption key that can be used to decrypt the encrypted information is itself encrypted with a group encryption key, and (c) a group decryption key that can be used to decrypt the encrypted first decryption key is accessible to the members of the group. In response to a request from a member of the group, the file server transmits the encrypted information and the encrypted first decryption key to the member.

As previously described herein with respect to independent claim 1, Ganesan does not teach or suggest transmitting, in response to a request from a client, (i) information that is encrypted with a first encryption key and (ii) a first decryption key that is usable to decrypt the encrypted information and that is itself encrypted with a second encryption key (i.e., a group encryption key), in which the second encryption key is associated with a second decryption key (i.e., a group decryption key) that is accessible to the client and that is usable to decrypt the encrypted first encryption key. Ganesan does not, therefore, teach or suggest the feature of claims 20 and 21 directed to *transmitting the encrypted information and the encrypted first decryption key to the member in response to a request from the member.*

Eldridge describes a data storage scheme in which a file server stores (i) a data file that is encrypted with a symmetric file key and (ii) the symmetric file key encrypted with a symmetric password key that can itself be decrypted by a quorum of users who request access to the data file. (Eldridge, Abstract.) Even if Eldridge does thereby suggest the *storing* feature of claims 20 and 21, Eldridge does not teach or suggest the *transmitting* feature of claims 20 and 21 because the Eldridge file server never transmits the data file to the quorum of users who request access to it. Indeed, as stated by the Examiner with respect to independent claim 21, Eldridge "fail[s] to show that in response to a request received at a file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said encrypted first decryption key encrypted with said group encryption key." Eldridge does not, therefore, teach or suggest the feature of independent claims 20 and 21 directed to

PATENTS
Attorney Docket No. SMY-219.01
P4421

transmitting the encrypted information and the encrypted first decryption key to the member in response to a request from the member.

In summary, neither Ganesan nor Eldridge teaches or suggests the feature of independent claims 20 and 21 directed to *transmitting the encrypted information and the encrypted first decryption key to the member in response to a request from the member.*

Independent claims 20 and 21 are therefore allowable. Since independent claim 21 is allowable, claims 22-30 depending therefrom are also allowable.

CONCLUSION

On the basis of the foregoing Amendment and Remarks, this application is in condition for allowance. Accordingly, Applicants request allowance.

Applicants invite the Examiner to contact the Applicants' Attorney should questions arise concerning this Response.

Respectfully submitted,

Date: May 18, 2004
Customer No: 25181
Patent Group
Foley Hoag, LLP
155 Seaport Blvd.
Boston, MA 02210-2600

Jeffrey M. Sears, Reg. No. 48,440
Attorney for Applicants
Tel. No. (617) 832-3022
Fax. No. (617) 832-7000